REMARKS

The present application was filed on June 20, 2003 with claims 1-16.

In the outstanding Office Action dated January 16, 2007, the Examiner: (i) objected to the drawings filed on June 20, 2003; (ii) rejected claims 1, 2, 4-6, 8-10, 12-14 and 16 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,697,488 (hereinafter "Cramer"); and (iii) rejected claims 3, 7, 11 and 15 under 35 U.S.C.§103(a) as being unpatentable over Cramer in view of a Cramer et al. article entitled "Multiparty Computation from Threshold Homomorphic Encryption" (hereinafter "Cramer paper").

In this response, Applicant amends independent claims 1 and 9. Applicant respectfully requests reconsideration of the present application in view of the amendments above and remarks below.

With regard to the objection to the drawings filed on June 20, 2003, the Office Action, at page 2, third paragraph, indicates that a PTO-948 form was attached with the present Office Action; however, no PTO-948 form was sent with the present Office Action. Applicant respectfully points out that the formal drawings filed on August 12, 2003 should correct any informalities objected to.

With regard to the §102(e) rejection, Applicants initially note that MPEP §2131 specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Applicants respectfully traverse the §102(e) rejection on the ground that the Cramer reference fails to teach or suggest each and every limitation of claims 1, 2, 4-6, 8-10, 12-14 and 16 as alleged.

Amended claim 1 is directed to a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of: obtaining the ciphertext in the first party device sent from a device associated with a second party; and generating in the first party device a plaintext corresponding to

the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme. Support for the amendment can be found at page 8, lines 1-9.

The present invention provides an efficient and provably secure protocol by which two parties, respectively designated herein as "alice" (or a first party) and "bob" (or a second party), each holding a share of a Cramer-Shoup private key, can jointly decrypt a ciphertext, but such that neither alice nor bob can decrypt a ciphertext alone. By way of one example, the invention can be used for a secure distributed third-party decryption service, which requires the joint agreement by two parties to decrypt a ciphertext. For example, this may be used to provide added security to: (1) a key recovery system by law enforcement, or (2) an "offline trusted third party" system in a fair exchange protocol. Another application involves techniques by which a device that performs private key operations (signatures or decryptions) in networked applications, and whose local private key is activated with a password or PIN (personal identification number), can be immunized against offline dictionary attacks in case the device is captured. Briefly, the goal of immunization against offline attack may be achieved by involving a remote server in the device's private key computations, essentially sharing the cryptographic computation between the device and the server.

Alice and bob obtain public and secret data through a trusted initialization procedure. After initialization, communication between alice and bob occurs in sessions (or decryption protocol runs), one per ciphertext that they decrypt together. Alice plays the role of session initiator in the decryption protocol. That is, alice receives requests to decrypt ciphertexts, and communicates with bob to decrypt these ciphertexts. We presume that each message between alice and bob is implicitly labeled with an identifier for the session to which it belongs. Multiple decryption sessions may be executed concurrently.

The Examiner in formulating the §102(e) rejection of claim 1 argues that each and every one of the above-noted limitations of claim 1 is anticipated by the teachings of Cramer. Applicants respectfully disagree.

Although Cramer at column 8, lines 25-35 refers to two devices, a sending device and a receiving device, the relied-upon portion of Cramer does not meet certain limitations of amended claim 1 as alleged. Cramer, at column 8, lines 25-35 states the following, with emphasis supplied:

> The computed ciphertext 30 with the cipher-number u_1, u_2, e, v is transmittable via an insecure channel, as described above. For the sake of clarity, this is not indicated in section III in FIG. 2. The ciphertext 30 does not leak any information about the keys and therefore the plaintext m is hidden assuming the Decisional Diffie-Hellman problem, also referred to as DDH problem, is hard. For the transmission of the ciphertext 30, the sending device, e.g. the first device 1 as described with reference to FIGS. 1a and 1b, uses output means, whereas the receiving devices, e.g. the second device 2 as described with reference to FIGS. 1a and 1b, uses input means for receiving the ciphertext 30.

Although the Examiner points to column 8 through column 10, line 5 as teaching or suggesting the generating step, the only reference to an exchange of information between the first and second devices is in the above quoted portion of Cramer, at column 8, lines 25-35. However, the relied-upon portion of Cramer discloses the two devices, the sending and receiving devices, interact solely to transmit the ciphertext from the sending device to the receiving devices. No where does Cramer teach or suggest the recited limitation of "generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. Again, as noted-above, the first and second devices can jointly decrypt a ciphertext, but neither can decrypt a ciphertext alone, such that the first and second devices communicate with each other to decrypt the ciphertexts, which Cramer does not disclose.

Accordingly, it is believed that the teachings of Cramer fail to meet the limitations of amended claim 1.

Independent claim 9 includes limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1. Independent claims 8 and 16, which recites limitations from the perspective of the second device, and include limitations similar to those of claim 1, are therefore believed allowable for reasons similar to those

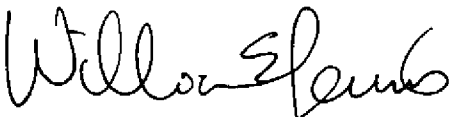
described above with reference to claim 1.

Dependent claims 2, 4-6, 10 and 12-14 are allowable for at least the reasons identified above with regard to claims 1 and 9. One or more of these claims are also believed to define separately-patentable subject matter over the cited art. Accordingly, withdrawal of the §102(e) rejection of claims 1, 2, 4-6, 8-10, 12-14 and 16 is respectfully requested.

With regard to the rejection of claims 3, 7, 11 and 15 as being unpatentable over Cramer in view of Cramer paper, Applicants assert that the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer. Thus, claims 3, 7, 11 and 15 are patentable at least by virtue of their dependency from claims 1 and 9. Claims 3, 7, 11 and 15 also recite patentable subject matter in their own right. Accordingly, withdrawal of the §103(a) rejection of claims 3, 7, 11 and 15 is respectfully requested.

In view of the above, Applicants believe that claims 1-16 are in condition for allowance, and respectfully request withdrawal of the §102(e) and §103(a) rejections.

Respectfully submitted,



Date: April 12, 2007

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946